PRIVACY IMPACT ASSESSMENT

Travel Document Issuance System (TDIS)

1. Contact Information

PIA Completed By: Name: Joyce France Title: PIA SME/IAE Org: CA/CST/ST Phone: 703-639-0384 Email: FranceJM@state.gov	**System Owner:** Name: Gerald L. Pascua Title: CA/CST Deputy Director and System Owner Org: CA/CST Phone: 202-485-7721 Email: PascuaG@state.gov
Program Manager: Name: Sharon B. Westmark Title: Program Manager Org: CA/CST/PSDD Phone: (202) 485-7722 Email: WestmarkSB@state.gov	**IT Security Manager:** Name: Edward F. Bacon Title: CA ISSO Security Branch Chief Org: CA/CST/ST/S Phone: (202) 485-7813 Email: BaconEF@State.gov
A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services	

2. System Information

(a) Name of system: Travel Document Issuance System

(b) Bureau: Consular Affairs

(c) System acronym: TDIS

(d) iMatrix Asset ID Number: 89

(e) Reason for performing PIA:

☐ New system – Logical Consolidated Boundary

☒ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance

(b) What is the security Assessment and Authorization (A&A) status of the system?

The system is currently in the Assessment and Authorization (A&A) process to receive an Authorization to Operate (ATO) status. TDIS is expected to receive an ATO by September 2020.

(c) Describe the purpose of the system:

TDIS supports the Bureau of Consular Affairs' mission requirements with respect to U.S. citizens who apply for passports domestically. TDIS was developed to provide assurance that applications for passports are processed in a timely manner; and that the production and issuance of machine-readable passports are properly managed in accordance with established Department of State (State Department) rules and regulations. TDIS is an integrated system utilizing both commercial-off-the-shelf (COTS) and customized hardware and software that is used by authorized State Department employees at passport agencies and centers. TDIS is the key application used for passport application/renewal processing at various passport agencies and processing centers around the country.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

TDIS contains PII on U.S. citizens and aliens lawfully admitted for permanent residence. The following PII is contained in TDIS: name, birthdate, gender, place of birth, social security number, phone number, personal address, email address, biometrics, business information, images, passport/ID numbers, substantive individual legal information, and substantive individual family information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 2651a (Organization of the Department of State)
- 22 U.S.C. 2705 (Documentation of Citizenship)
- 22 U.S.C. 211a-218 (Passport Application and Issuance)
- 22 U.S.C. 3927 (Chief of Mission)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide SORN

STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

☒Yes
☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

Schedule number Department of State Records Disposition Schedule:
A-13-001a, b, c &d: Passport Records; Passport and citizenship Case Files
Description: Case files containing; passport applications, reports of birth of American Citizens Abroad; certificates of Witness to Marriage, Applications for Amendment or Extension of Passport; certificates of loss of nationality; and other supporting forms, documents and correspondence pertaining to each case.
Disposition: The length of time records will be kept is dependent on the specific item and the applicable disposition rules in A-13-001a, b, c & d, of the State Department records retention schedule.
DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05 respectively.

A-13-001-21a, b, c&d Travel Document Issuance System (TDIS)
Description: TDIS is a computerized system used to process passport applications at Passport Agencies in the United States.

Disposition: The length of time records under these schedules kept is dependent on the specific item and the applicable disposition rules in A-13-001-21a, b, c&d, of the State Department records retention schedule.
DispAuthNo: N1-059-96-05

A-13-001-23 - Routine Passport Application Status Check and Expedite Fee Upgrades E-mail
Description: Email messages regarding the status of passport applications and requests for expedited service.
Disposition Temporary: Destroy/delete when 25 days old
DispAuthNo: N1-059-98-03, item 1

A-13-002-02 Requests for Passports
Description: Copies of documents relating to selected passport requests.
Disposition: Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 2

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 3

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☐ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

26 U.S.C. 6039E - Information Concerning Resident Status

22 U.S.C. § 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

TDIS cannot be not accessed by the public. The applicant completes the required form for a passport or a passport renewal either online or via a CA/Consular Systems and Technology (CST)

system, where information is transmitted to TDIS for processing by TDIS post analysts. Information is also collected via hard copy of the completed form and taken to the agency or center where State Department employees input the data into TDIS.

Information is collected by the following forms:

DS-11: "Application for a U.S. Passport"
DS-82: "Application for Passport by Mail: Renewal"
DS-5504: "Passport Re-application (Changes/Corrections to a Current Valid Passport)"
DS-64: "Statement Regarding Lost or Stolen Passport"
DS-4085: "Application for Additional Vis Pages or Miscellaneous Passport Services"

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

Accuracy of the information on passport applications and supporting citizenship evidence is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage of the passport process by State Department analysts, in addition to information being cross-checked with other CA systems to minimize instances of inaccurate data.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Passport applicants are responsible for ensuring that the passport application information is current at the time of submission. Quality checks are conducted against the submitted documentation at every stage of the passport process. Administrative policies are established for currency and accuracy of information by which State Department analysts perform checks and reviews. Data from applications that is entered into TDIS by analysts is also checked against other CA/CST systems for currency and inconsistencies. These CA/CST systems consist of the Front End Processor (FEP), Consular Affairs Enterprise Service Bus (CAESB), Consular Data Information Transfer System (CDITS), Electronic Passport Application Form Internet Website (2BD), Overseas Consular Support Applications (OCSA), Passport Information Electronic Records Systems (PIERS) and Consular Consolidated Database (CCD).

(g) Does the system use information from commercial sources? Is the information publicly available?

Yes, TDIS uses commercial information from Citi Bank (referred to as CITI) that is transferred to TDIS by the Consular Data Information Transfer System (CDITS). The information transmitted by CITI is not publically available.

(h) Is notice provided to the individual prior to the collection of his or her information?

TDIS does not collect information directly from applicants and is not accessible by the public. Passport applications whether in paper or electronic form contain Privacy Act Statements, and notice and consent are provided at the collection point.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

☐Yes

☒No

- If yes, how do individuals grant consent? If no, why are individuals not allowed to provide consent?

TDIS is not a customer-facing application and therefore does not collect information directly from the public. Consent is provided when the applicant completes and submits the forms listed in 4(c).

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII listed in Question 3d is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function of providing passport application/renewal processing services.

5. Use of information

(a) What is/are the intended use(s) for the information?

The PII is used to provide passport services to applicants applying for or renewing passports.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The PII is used according to the purpose for which the system was designed which is to process requests for new and renewed passports.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

TDIS does not analyze information.

(2) Does the analysis result in new information?

☐Yes

☒No -

(3) Will the new information be placed in the individual's record?

☐Yes –

☒No –N/A

(4) With the new information, will the State Department be able to make new determinations about the individual that would not have been possible without it?

☐Yes -

☒No – N/A

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The term "internal sharing" traditionally refers to the sharing of information with the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the TDIS system is shared internally with other CA systems FEP, CAESB, CDITS, 2BD, OCSA, PIERS and CCD as mentioned previously.

Externally, TDIS information may be disclosed to external Federal agencies such as the Department of Homeland Security, Treasury, Social Security Administration as well as State and local agencies such as law enforcement or tax agencies. Information may also be disclosed to attorneys representing an individual in administrative or judicial passport proceedings when the individual to whom the information pertains is the client of the attorney making the request.

(b) What information will be shared?

Any and all information identified in paragraph 3d.

(c) What is the purpose for sharing the information?

The PII is used internally to facilitate processing of passport requests and renewals. External sharing of information is used to adjudicate the processing of the passports.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal Sharing: TDIS information is shared database to database among CA/CST systems and is transmitted via Transmission Control Protocol/Internet Protocol (TCP/IP) network. This is a secure transmission method permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

External sharing: TDIS information is not interconnected with external offices or agencies, but shares information by other means, e.g., files, email, or other CA systems having information on an individual's history, nationality, or identity.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal Sharing: Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing of information and disclosure including, but not limited to, annual security training, separation of duties, least privilege assignments and personnel screening.

Safeguards in place for internal sharing include secure transmission methods (methods detailed at end of this section) permitted by State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

External Sharing: Memorandums of Understanding (MOU/MOA) are in place with other government agencies regarding the use and handling of information

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

Accidental disclosure of information to non-authorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

These risk areas are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, sensitive but unclassified, and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) **What procedures allow individuals to gain access to their information?**

TDIS is not a public facing system and does not obtain information directly from applicants. Applicants can follow instructions for gaining access as stated in SORNs STATE-26 and STATE-05. They may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access by contacting the listed offices by phone or by mail.

(b) **Are procedures in place to allow an individual to correct inaccurate or erroneous information?**

☒Yes ☐No

If yes, explain the procedures.

TDIS does not obtain information directly from applicants. In order to correct inaccurate or erroneous information, applicants may contact the representative who initially assisted them with their applications. Additionally, applicants can follow instructions for requesting changes to their information as stated in SORNs STATE-26 and STATE-05 which are available on the Department of State Privacy Act/FOIA web site. They may also visit the Department of State Privacy Act/FOIA web site for the Privacy Policy which includes instructions on how to request changes by contacting the listed offices by phone or by mail.

(c) **By what means are individuals notified of the procedures to correct their information?**

Individuals are notified of the procedures to correct records that feed information into TDIS by a variety of methods: during their interview; after, applicants can contact the representative who assisted them; published SORNs STATE-26 and STATE-05; Department of State Privacy Act Website; link on web pages to Department of State Privacy Policy; instructions on forms or web pages where the data was input; or being notified by letter or email that a correction is needed

Each method contains information on how to amend records and who/what office to contact and the contact information.

If no, explain why not.

8. Security Controls

(a) How is the information in the system secured?

TDIS is secured within the Department of State internal network where risk factors are mitigated through the use of defense in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform their official duties.

Access to TDIS is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system. TDIS audit logs may be derived from data such as event identifier, date, time and

event type, user account and computer name. Audit trails are reviewed daily for suspicious activities, which are reported to senior management immediately.

TDIS is configured according the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Each authorized TDIS user must be approved by the supervisor and sign the user access agreement/rules of behavior before being given an OpenNet user account and access to TDIS. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon to TDIS specifically.

Access to TDIS is role based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information to be accessed by individuals. Security officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(d) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information (PII). In accordance with Department of State Security Configuration Guides, TDIS auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the TDIS audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual security training (PS800 Cyber Security Awareness) is required for all authorized users of TDIS. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. Government employees accessing TDIS must also complete the one time Privacy PA459 course entitled, "Protecting Personally Identifiable Information." In addition to the above required training, the Passport Services Internal Control Guide requires all personnel (government and contractors) to complete the Passport Data Security Awareness (PC441) course as an annual recertification to maintain access to TDIS. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.

The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require all users to sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

TDIS data in transit uses Transmission Control Protocol/Internet Protocol (TCP/IP) for data transport. The data in transit is encrypted and consist of multiple layers of protocols to assist in the integrity of data transmission and information integrity. Auditing techniques are also used to monitor and record possible attempts at unauthorized access.

(f) How were the security measures above influenced by the type of information collected?

Exposure of an individual's PII may lead to inconvenience, distress, or damage to standing or reputation, financial loss, harm to State Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above in paragraph 8(a-e) were implemented to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

Department of State authorized users of TDIS, CST Administrators, System Administrators, and Database Administrators have access to the data in the system.

TDIS authorized users include both government and contract employees. Users can view all data; however, there are restrictions as to what data each user can change or update based on their roles.

(b) How is access to data in the system determined?

Access is role based and users are granted only the role(s) required to perform officially assigned duties. Role-based access requests are approved by the supervisor and local ISSO.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Information is documented in the System Security Plan. The TDIS Plan includes procedures regarding system access to data in this specific system.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No, all users will not have access to all data in TDIS. Only the system and database administrators have access to all data in the system to perform their duties.

Department of State authorized users of TDIS:

TDIS Post users: All TDIS Post users can view data; however, there are restrictions as to what data each user can change and update.

CST Administrators: The CST Administrators are responsible for creating accounts within CST and assigning the appropriate application roles. Post users are frequently limited to viewing the data for their own post.

System Administrators: The System Administrators include both government employees and contractors. System Administrators are responsible for all daily maintenance, establishing access control lists (ACLs), and backups. The duties of system administrators require that they be granted system administrator privileges to the respective application servers. The respective post authorizes the establishment, activation, modification, review, disabling, and removing of System Administrator accounts.

Database Administrators: Database Administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configuration, to the database.

DBA access is controlled by the Integrated Services (IS) team through the use of ACLs as established by the system administrators.

Separation of duties and least privilege is employed, and users have access to only the data that the supervisor and local ISSO approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and automated access enforcement mechanisms control access to PII in TDIS.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges in TDIS are restrictive rights/privileges or accesses needed by users for access and the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN) in TDIS.

-Privacy training informs users of the Rules of Behavior and warns against unauthorized browsing.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.